ARTICLE APPEARED
ON PAGE 1A

USA TODAY
26 October 1983

COVER STORY

Spy case shows holes in our security

"Certainly not single event;" 'system is only as good as the people involved in it

By Richard Price
USA TODAY

The USA has a hot-new spy thriller, starring a globe-trotting American engineer who allegedly sold secrets to the Soviet Union — secrets allegedly stolen with the help of his late wife.

Accused is James Durward Harper, Jr. 49, who was denied bail Wednesday. But as the investigation continues, his alleged role may take second place to that of his wife, Louise Schuler Harper, a secretary who held a "Secret" security clearance at Systems Control Inc. in Palo Alto, Calif.

The FBI says that until she died of cirrhosis last June, Louise Harper went with her husband into the building on nights and weekends to browse through classified information on items like the Minuteman missile.

Some people don't believe it. "If there is anybody guilty in this, it isn't Louise," said Jay Politzer, a former assistant to the company chairman. But Mrs. Harper's alleged role is important to security specialists because it shows the difficulty of protecting secrets handled by many.

■ More than 208,000 American civilians have security clearances and access to classified material at companies holding government contracts.

■ There are more than 11,000 such companies around the USA, and the walls around many of them may be growing more porous. Last year, the Defense Investigative Service, the government's overseer of security, conducted 40,000 espionage investigations of company employes — double the number in 1975.

"This is certainly not a single event," Harry V. Martin, publisher of *Defense Systems Review*, said of the Harper case. "It goes on frequently."

Companies must protect themselves — consider Raytheon Co. of Lexington, Mass., a diversified electronics manufacturer that does 40 percent of its $5.5 billion in sales with the government. File cabinets have red warning signs that flash when they're left unlocked; copying machine is stamped with a reminder of the criminal penalties for copying classified information; most government work is carried on in separate buildings surrounded by chain link fences.

"The world is indeed different," says Fred Haynes, an associate director of the National Technical Information Service in Washington, D.C. "As soon as you put on your security clearance, it's like putting on a cloak of responsibility."

Security rules are laid out in what defense contractors call their "bible" — the 343-page *Industrial Security Manual for Safeguarding Classified Information*.

It's a blueprint for a world of color-coded badges, vaults, steel canisters, electronic screening devices, release forms and labels on every document warning who is allowed to read what.

Among the instructions:

■ Employes should receive periodic "counter-intelligence briefings" warning them to be wary of "gladhanding strangers . . . who could prove to be the "proverbial wolf in sheep's clothing."

■ "The neighbor who you might meet at a PTA meeting . . could be a fellow American who has been recruited as an agent by a hostile service."

■ Locks on classified material should be changed at least once a year.

■ Never use fewer than two witnesses when destroying classified material.

■ Top Secret material must be examined by a guard every two hours — and buildings with classified material must be guarded 24 hours a day, every day.

■ Follow thousands of code words; "Top Secret" is the wrong term for material concerning NATO. The right term: "Cosmic Top Secret."

But rules are one thing, enforcement another — not an easy task for the Defense Investigative Service.

With a budget of $106 million and a staff of 3,468, the Pentagon agency must do more than chase allegations of espionage. It must inspect 12,500 installations at least once a year — and frequently three times. It also does more than 2.39

CONTINUED